Cassandra Crossing/ Zombie Computing

(305) - Cosa si nasconde nel BIOS di numerosissimi computer? Perché certe funzioni sono presenti su tutte le macchine ad eccezione di…

Cassandra Crossing/ Zombie Computing

Figure 1:

(305) - Cosa si nasconde nel BIOS di numerosissimi computer? Perché certe funzioni sono presenti su tutte le macchine ad eccezione di quelle destinate ai militari? Il Trusted Computing non è affatto morto.

6 dicembre 2013—C'era una volta il Grande Fratello tecnologico: faceva tanta paura a tutti e si chiamava Palladium, poi Trusted Computing, poi TC, poi…

Poi, proprio come la "Total Information Awareness" di Bush, apparentemente è sparito. Nessuna delle due iniziative in realtà è sparita: la TIA è diventata quello che il Datagate ha svelato, il TC è stato implementato ma viene usato poco: in compenso ha prodotto "figli" nuovi ed interessanti, più semplici e più pericolosi.

Nemmeno Cassandra ha più parlato di Trusted Computing, ed il motivo è semplice: per quanto detto sopra non è più un grosso pericolo.

Non è che il Trusted Computing sia diminuito di importanza, ma piuttosto che alcuni suoi figli spirituali sono diventati molto più pericolosi del loro "babbo", e contemporaneamente la maggior parte del Popolo della Rete ha cominciato a comportarsi in maniera totalmente idiota come Pinocchio nel Paese dei Balocchi, dedicando ore ed ore al giorno a far del male a sé ed agli altri via comunità sociali.

Questi signori inoltre spendono molti soldi per comprarsi device permanentemente connessi alla Rete, che finiscono in ogni tasca ed in ogni casa (una volta si chiamavano oggetti con canale di ritorno connessi a formare l'Internet degli Oggetti).

Ma la storia che Cassandra oggi vi vuole parlare è perversa, semplice, economica, e giace appena appena nascosta sotto il pelo della Rete.Per raccontarla purtroppo, Cassandra necessita di una lunga (ma comunque utile) lezioncina tecnica.

I computer sono da sempre dotati (beh, diciamo negli ultimi 30 anni sicuramente, l'ENIAC o lo Z4 non l'avevano) di un software (o meglio, di un firmware) chiamato BIOS, che si preoccupa di diverse cose che avvengono appena si accende il computer, tipo fare la diagnostica della scheda, permettere alcune regolazioni all'utente, e caricare ed eseguire il boot block per eseguire il boot del sistema operativo.

20 anni fa i BIOS del pc erano semplici, stavano in 256 Kb, ora ci sono delle schede madri (e dei laptop) che hanno chip da 4 GB. Cosa c'è in questo spazio?

Sicuramente BIOS più complessi e performanti, che permettono di aggiornare il BIOS stesso senza dover cambiare fisicamente il chip. Esiste addirittura una motherboard di una famosa azienda che contiene nel BIOS una versione ridotta di una nota distribuzione GNU/Linux, permettendo all'utente di collegarsi ad internet con un browser anche con disco collassato e senza usare alcun cd o chiavetta USB.

Ma, come si dice, "il demonio sta nei dettagli", e nella nostra storia il nodo viene al pettine per quel fatto di poter aggiornare il BIOS.

Cosa succede se va via la corrente mentre si effettua l'aggiornamento? Beh, una volta bisognava reinviare la scheda od il laptop in fabbrica. Poi le azienda hanno creato nel chip del BIOS una zona che l'utente non può riscrivere, la quale contiene il programma per effettuare l'aggiornamento del BIOS. In questo modo un aggiornamento fallito non distrugge il programma stesso e si può ritentare.

Buona idea! Peccato che la si possa estendere inserendo in questa zona del BIOS a sola lettura qualsiasi software il costruttore desideri, che l'utente è costretto a tenersi, e che non necessariamente è una sana distribuzione GNU/Linux, ma in linea di principio qualsiasi software: anche qualche malware, virus o trojan.

Cassandra chiede scusa di questa lunga digressione, ma siamo arrivati al punto.Esistono ormai da anni software dedicati esclusivamente al recupero di computer e smartphone rubati che, valendosi delle gagliarde capacità della moderna ferraglia, gridano appena il ladro si connette e ce lo segnalano con tanto di coordinate GPS o foto scattate con la telecamera. Storie vere, funzionalità in effetti potenzialmente utili, specie quando si è distratti o non si utilizza un buon cavo d'acciaio.

Ma una nota azienda che produce software di sicurezza da tempo pubblicizza un prodotto che, oltre ad agire come rintraccia-ladri, ha l'interessante proprietà di non poter essere disinstallato nemmeno formattando il disco od addirittura sostituendolo.

Viene appunto scritto nella zona a sola lettura del BIOS con la complicità in accordo con un sorprendente numero di costruttori di pc.

Ora andrebbe ancora tutto bene, ognuno sul computer che fabbrica ci mette quello che gli pare, tanto l'**utonto** utente medio può già farsi tutti i danni che ritiene in tanti altri modi, perché normalmente non si interessa a cosa c'è già dentro al computer, al sistema operativo ed alle applicazioni che acquista.

Cassandra è invece sanamente paranoica, e per questo si è informata sulle modalità di funzionamento dell'oggetto di cui sopra, scoprendo cose decisamente preoccupanti.

Nel caso di cui parliamo, la suddetta azienda di sicurezza ha appunto inserito nel BIOS il suo software di tracciamento del computer, che si trova in una modalità disattiva per default. Sta lì perché la suddetta azienda ha stretto accordi commerciali con un numero impressionante di costruttori, e la lista dei laptop attualmente in vendita, contagiati dotati di questo software è impressionantemente lunga.

Quello di Cassandra per fortuna no!Cosa avviene in pratica? Chi vuole attivare questa feature di tracciamento del laptop, compra (e paga) un client software che attiva la parte esistente (e non modificabile) nel BIOS.

Da questo momento essa prende il controllo del sistema, ed è in grado di reinstallare il client stesso anche se viene reso inattivo o cancellato, se il disco viene formattato o addirittura sostituito.

Non è chiaro se questo avvenga perché il client è contenuto nel firmware stesso o perché il firmware riesca addirittura a connettersi ad Internet e scaricarlo dal sito del produttore. Ambedue le ipotesi fanno paura, e vediamo perché.

In questa situazione il PC è zombificato, perché le utili funzioni di tracciamento antiladro non possono essere disattivate dal ladro, ma nemmeno dall'utente.

Eventuali funzioni nascoste del software, ovviamente rigorosamente proprietario, possono in linea di principio fare qualsiasi cosa e sono altrettanto inamovibili.

L'azienda di sicurezza fornisce ovviamente il servizio di disattivazione del software, che riporta il pc nella situazione in cui si trovava al momento dell'acquisto, cioè di firmware "dormiente". Anche i vampiri di giorno dormono…

Fin qui, si fa per dire, ancora tutto bene.Ora poniamo alcune considerazioni, anzi domande la cui risposta è lasciata al lettore.Perché questa iniziativa poco nota al pubblico, guardando la lunghezza della lista dei laptop supportati, ha avuto così tanto successo presso i costruttori?

Chi garantisce che il client fornito faccia solo quello che viene dichiarato nella scheda tecnica?

Chi garantisce che questo firmware non possa essere attivato automaticamente da software malevoli, siti web compromessi, terze parti o tecnocontrollori vari all'insaputa dell'utente, potendo in questo caso ovviamente svolgere anche funzioni ben diverse dal tracciamento antiladro?

E, "dulcis in fundo" ("in fundo" alla lista dei device supportati) perché c'è scritto "*All models are supported except XXXXXX Military version*".

Forse che i militari sono più furbi e non vogliono zombie in mano ai loro soldati? Caro Giulio, non sarà che la tua vecchia massima sul diffidare è più che mai applicabile in questa situazione?

Rimane solo da decidere come chiamare questo tipo di hardware/firmware.Trovato! il Trusted Computing ha anche utilizzi positivi, questo merita senz'altro il nome di "Untrusted Computing".

Stateve ***accuorti***.

Originally published at punto-informatico.it.